U.S. Department of State Foreign Affairs Manual Volume 5 Handbook 2
Telecommunications Handbook

5 FAH-2 H-620
NON-SECURE CIRCUITS

(CT:TEL-32;   06-25-2012)
(Office of Origin: IRM/BMP/GRP/GP)
(Updated only to revise Office of Origin and some formatting)

5 FAH-2 H-621 MAINTENANCE

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

Non-secure telephone equipment must be procured, installed, and maintained in accordance with security standards appropriate to the technical threat level of the post. Specific maintenance procedures depend on the type of telephone system and level of training of IPC staff. All posts abroad should follow the general guidelines below and develop specific procedures unique to post's needs:

(1)   Document post's procedures; update the PBX programming records; and keep them on file in the IPC;

(2)   Swap defective components immediately with operable spares and send defective components for repair and return in accordance with 5 FAH-2 H-621.5;

(3)   Stock enough spare components to keep the system continually and fully operational. As a minimum, one spare for each unique telephone item in post's inventory and multiple spares for a larger volume of like items;

(4)   Update the Worldwide Property Accountability System (WPAS) inventory when parts are sent to the Department for repair and when replacements are received at post;

(5)   Instruct users in the capabilities of their telephone sets to improve the efficiency of their operations; and

(6)   Maintain the operational status of call accounting systems, if used.

5 FAH-2 H-621.1 Controlled Access Areas

(CT:TEL-12;   03-08-2005)
(Uniform all agencies)

The following security standards govern the maintenance and daily operations of telephone equipment and circuitry located inside controlled-access areas (CAAs) of all Department facilities, regardless of threat level. See 12 FAH-6 H-311.4, OSPB Security Standards and Policy Handbook, for additional, threat-specific security standards:

(1)   Only TOP SECRET-cleared U.S. citizens may maintain telephones used in CAAs;

(2)   Instruments used in CAAs must be TSG-approved or installed with TSG-approved disconnect devices;

(3)   The post Counter-Intelligence Working Group (CIWG) must approve private or direct outside lines that are not administered through a PBX. Such telephones must be installed with a TSG-approved disconnect at the point of telephone wire entry into the CAA;

(4)   Telephone equipment for CAAs must be transported to *the* site by secure transport under 24-hour control of Secret-cleared U.S. citizens or by appropriate U.S. Government-approved technical means and seal. Store equipment in CAAs within a locked and alarmed area or place equipment in secure storage protected by a cleared U.S. presence on a 24-hour basis;

(5)   DS prohibits non-secure cellular telephones and convenience telephone accessories, such as speaker phones, cordless telephones, and stand-alone answering machines;

(6)   DS and IRM must approve optional features of a PBX, such as voice mail, auto attendant, and call distribution, prior to implementation;

(7)   PBX and main distribution frames (MDFs) for telephones installed inside a CAA must be located in a CAA or within a locked and alarmed room; and

(8)   IPC must control access to IDFs that support telephone instruments or circuits in the CAA.

5 FAH-2 H-621.2 Outside Controlled-Access Areas

(CT:TEL-12;   03-08-2005)
(Uniform all agencies)

Unescorted Foreign Service Nationals (FSNs) may repair and maintain telephone circuitry and instruments located outside CAAs. FSN access to the PBX and MDF may be prohibited or limited to escorted access. The RSO makes the determination, as appropriate, in accordance with 12 FAH-6, OSPB Security Standards and Policy Handbook, and the DS-assigned technical threat level.

5 FAH-2 H-621.3 Remote Maintenance Restrictions

(CT:TEL-12;   03-08-2005)
(Uniform all agencies)

a. Remote maintenance, also referred to as remote maintenance administration and test (RMATS); remote diagnostic services (RDS); and centralized maintenance allows a remote site to access local PBX software and perform maintenance diagnostics and polling and programming functions. These functions may be performed only with the concurrence of the post. Post must be made fully aware of any reconfiguration or changes that are proposed to its PBX. In a diagnostic and corrective action scenario, it is understood that the action required may not be known in advance; however, a complete recapitulation of the actions taken must be provided to post when the maintenance or restoral action has been completed.

b. Routine remote maintenance or diagnostics may be conducted only from cleared facilities over secure communications links.

c. In an isolated instance, if a remote maintenance procedure over an unsecured communication link is necessary, it may be provided by an uncleared facility over a non-secure communication link. This provision also applies if the technical ability for a secure link does not exist at a particular post. If remote maintenance (RMATS) is performed over an unsecured link, the following restrictions must be adhered to:

   (1)   The RMATS facility must not be able to access the PBX except through a port dedicated to infrequent RMATS activity;

   (2)   Unless in use, the RMATS port must remain disconnected from all

trunks and lines leaving the PBX room. If modems are required for

RMATS, they must be disconnected from the RMATS port when not in use; and

(3) Initiation of an RMATS activity and the connection between the RMATS port and the RMATS facility must be by an authorized person from within the PBX.

d. IPC personnel should be familiar with the post's PBX remote maintenance capability. However, in those posts where there is no Information Management Specialist assigned or IPC personnel have not been afforded the opportunity to obtain specific PBX training, the remote facility conducting the RMATS, RDS, or centralized maintenance activity is still required to obtain concurrence from the responsible party at post. IPO should consult IRM/OPS/ITI/LWS/FPT to ensure that post's PBX is configured to allow remote maintenance under the security restrictions approved by DS.

5 FAH-2 H-621.4 Direct Inward System Access (DISA)

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

The DISA feature of PBX programming must be disabled. If uncertain about how to disable this feature or confirm that it is disabled, consult the area RIMC or IRM/OPS/ITI/TWD/FPT.

5 FAH-2 H-621.5 Repair and Return Procedures

(CT:TEL-12;   03-08-2005)
(Uniform all agencies)

a. The repair of Classified Information Processing Equipment (CIPE), radio, and telephone systems will all be handled in a similar manner, the same process that has been in place for ADP equipment located inside the CAA. Post will send an official telegram to USOFFICE ITECH WASHDC, SECSTATE WASHDC and the appropriate RIMC. This telegram should be assigned TAGS AMTC, ACOA, and KRIM. A slug line must be included for the Customer Service Exchange Activity (IRM/OPS/ITI/LWS/MNT/CSEA), the respective regional bureau, and the cognizant maintenance provider:

CIPE/ADP	-	IRM/OPS/ITI/LWS/MNT
Radio	-	IRM/OPS/ITL/LWS/RPB
Telephone	-	IRM/OPS/ITI/LWS/FPT

b. The telegram should request a "Return Authorization Number" (RAN) and provide registry number, model number, and serial number of equipment requiring repair. CSEA will then provide the RAN so that post may return the equipment. All equipment should be returned to:

> U.S. Department of State
> SA-21, IRM/OPS/ITI/LWS/MNT/CSEA
> 7500 Boston Blvd.
> Springfield, VA 22153

c. Posts must request a RAN prior to returning the equipment. This allows time for LWS to obtain regional bureau clearance for repair or replacement of the faulty equipment. This includes equipment being sent back for warranty repair, since that does incur a handling expense and the regional bureaus must be able to track all expenses.

5 FAH-2 H-622 CALL ACCOUNTING

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

a. A call accounting system is an effective method to track recurring calling patterns, to ensure that users comply with policies for placing official calls, and to determine costs of calls. Detailed call accounting information must be safeguarded and disseminated only on a need-to-know basis according to 12 FAH-6, OSPB Security Standards and Policy Handbook.

b. Post management and the ranking IRM officer determine post's need for a call accounting system. The IRM officer should consult the RIMC to decide which type of call accounting system to procure and for current vendor information.

5 FAH-2 H-623 PROCUREMENT

5 FAH-2 H-623.1 PBX

(TL:TEL-2;   05-23-2002)
(Uniform State only)

The senior IRM officer at post consults with the RIMC and post management to decide when to replace a PBX. The IRM officer submits the formal request for funding the PBX in the IRM Section of post's Mission Performance Plan. The request must include estimates for the total cost of the equipment and installation and address the justification criteria below:

(1)   Capacity of current PBX for expansion with regard to a projected increase in the number of users, instruments, or telephone lines;

(2)   Age, reliability of equipment, availability of spare parts;

(3)   A change in security standards applied to post;

(4)   Change in business needs linked to the Department's regional bureaus or post's mission; and

(5)   Measurable improvement in efficiency of a new system over an existing system, i.e., automated functions to replace human resource requirements.

5 FAH-2 H-623.2 Procurement Responsibility

(CT:TEL-12;   03-08-2005)
(State only)

a. Coordinate all procurement requests with RIMC and IRM/OPS/ITI/TWD/FPT. IRM/OPS/ITI/TWD/FPT will organize a needs assessment survey conducted by RIMC and FPT representatives, in consultation with post management and the ranking IRM officer. FPT will then coordinate procuring, shipping, inventorying, and installing the new system with RIMC and post's IRM officer. A/LM/OPS/WLC/MAT is responsible for ordering telephone equipment, from the central investment fund for major post PBX upgrades, or bureau and/or post funds for ancillary systems or individual components. Once funding is provided, A/LM/OPS/WLC/MAT will submit the order for the post and advise the vendor of the method for shipment as prescribed by the post.

b. If the vendor is to ship the equipment via Department shipping channels, A/LM/OPS/WLC/MAT must concur, and funds must be provided to cover the cost of shipment from SA-21. A/LM/OPS/WLC/MAT will not accept equipment from vendors that was purchased by posts unless they have previously received copies of formal purchase requests or telegraphic orders. The correct address for shipping through Department channels is:

Department of State
(Post Name)
A/LM/OPS/WLC/MAT
7958 Angus Court, SA-7b
Springfield VA 22153

5 FAH-2 H-623.3 Supplemental Components

(TL:TEL-2;   05-23-2002)
(Uniform all agencies)

Post must fund call accounting systems, telephone sets, replacement circuit cards, PBX expansion cards, and other supplemental telephone components. Coordinate all procurement requests with RIMC and IRM/OPS/ITI/TWD/FPT. RIMC will ensure that supplemental components are compatible with post's telephone system and advise if the Department provides maintenance support for proposed purchases. A/LM will track the purchase order from the Department side through receipt at post and ensure that items are properly bar-coded and sent to post through the appropriate pouch channels.

5 FAH-2 H-624 THROUGH H-629 UNASSIGNED